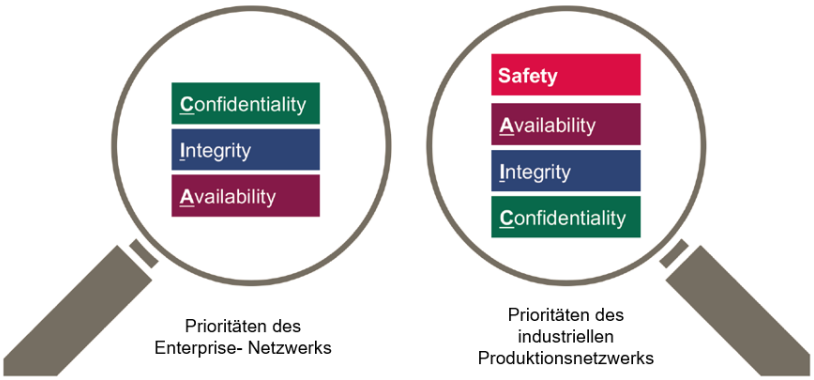
Bedrohungsschutz für kritische IT-Netzwerke.

Advanced Threat Protection, Security and Compliance for Critical IT-Networks.

Die Sicherheitsbedürfnisse der Enterprise-Umgebung ihres IT-Netzwerks unterscheiden sich generell von denen der Industrie- und Produktions-Umgebung.

Der bedeutendste Unterschied: Automatisch ausgelöste Veränderungen in der System-Konfiguration (z.B. das automatische Blockieren von Datenverbindungen) können einen ungewollten Produktions-Unterbruch verursachen und sind daher nicht praktikabel.



Confidentiality = Vertraulichkeit / Integrity = Vollständigkeit / Availability = Verfügbarkeit / Safety = Sicherheit

Voraussetzungen für eine erfolgreiche Sicherheits-Lösung

	Praxisorientiert. Die Lösung muss Bedürfnisse aus der Industrie zugeschnitten, leicht umsetzbar und von «nicht Security-Experten» bedienbar sein.
	Real World Die Lösung muss die tatsächlichen Gegebenheiten abbilden und den realen Bedrohungen für industrielle Produktionsnetzwerke entsprechen.
	Vollständig Die Lösung muss Durchgängig alle Sicherheits-Bedürfnisse abdecken.

INDUSTRIAL CYBERSECURITY

NETWORKCOMPETENCECENTER
by YELLO NETCOM & DDS NETCOM

Praxisorientiert: Wir realisieren Lösungen, die auf die besonderen Anforderungen und Prioritäten von Industrie- und Produktionsnetzwerken zugeschnitten sind. «Angepasste» Enterprise-Lösungen können selten erfolgreich implementiert werden.

Real World: Wir realisieren Lösungen, die Ihre eigenen Prioritäten bezüglich Sicherheit, Verfügbarkeit und Zuverlässigkeit abbilden, weil nur Sie über Ihre Produktionsprozesse und deren elektronischen Hilfsmittel im Bilde sind.

Vollständig: Wir kennen die Konvergenz zwischen dem Enterprise- und Ihrem industriellen Produktionsnetzwerk und somit die Notwendigkeit einer vollständigen und gesamtheitlichen Sicht auf die Cybersecurity Ihrer Organisation. Ohne diese duale Perspektive wird sich die Lücke zwischen Enterprise- und Produktionsnetzwerk vergrössern, was sich schlussendlich negativ auf das gesamte Sicherheitsniveau auswirkt.

Drei Schritte zu einem sicheren Produktions-Netzwerk

1 Secure Industrial Networks	2 Secure Industrial Endpoints	3 Secure Industrial Controllers
- Segmentierung - Identifizierung von Zonen und Leitungen - Überwachung und Alarmierung - Wireless und Remote-Access - Allgemeine Bedrohungsbegrenzung	- Inventarisierung - Identifizierung von verwundbaren Endpunkten - Sichere und autorisierte Konfigurationen - Verhindern von unautorisierten Änderungen	- Durchgängiges Änderungsmanagement - Schutz von verwundbaren Steuerungen mit verwertbaren Informationen - Sichere, autorisierte und überwachte Zugriffe

Unsere Lösungen

Angriffsfläche reduzieren	Unsere Lösungen trennen Ihre kritische IT-Infrastruktur vom Enterprise-Netzwerk, ohne die Durchgängigkeit der auf beiden Seiten benötigten Daten zu reduzieren. Wir segmentieren und überwachen Ihre kritische IT-Infrastruktur, indem wir unterschiedliche Sicherheitszonen bilden und unautorisierte Dienste und Geräte in Ihrem Netzwerk identifizieren.
Sicherer Remote-Access	Unsere Lösungen implementieren einen sicheren Zugriff auf Ihre kritische IT-Infrastruktur, identifizieren alle Zugriffe von aussen, validieren die Konfigurationen der Remote-Access- Produkte und überwachen diese automatisch, um das Einhalten ihrer diesbezüglichen Richtlinien jederzeit sicherzustellen.
Sichere Authentifizierung	Wir richten an allen Endgeräten eine sichere Authentifizierung ein. Unsere Lösungen validieren und überwachen automatisch alle diesbezüglichen Konfigurationen. Zudem detektieren sie automatisch Änderungen bezüglich der Zugriffsrechte von Benutzern und die Stärke der Passwörter gemäss ihren Richtlinien.

DDS NETCOM AG I ALLMENDSTRASSE 8 I CH-8320 FEHRALTORF | TEL. +41 43 355 22 11 I FAX. +41 43 355 22 10 I www.dds.ch
YELLO NETCOM GmbH | Birkenallee 115-117 | D-48432 Rheine | TEL. +49 5971 96176 0 | FAX. +49 5971 96176 25 | www.yello-net.de

Sicherstellen von richtigen Konfigurationen und Patches.	Wir implementieren kein Patch-Management-System, überwachen aber dessen richtige Funktion, indem wir sicherstellen, dass alle Netzwerkteilnehmer die richtigen Patches verwenden. Zudem können wir unerlaubte Änderungen und ungepatchte Teilnehmer identifizieren.
Application Whitelisting	Mit unseren Lösungen administrieren und überwachen Sie alle Ports, Dienste, Benutzer und Applikationen auf Ihrer gesamten kritischen IT-Infrastruktur, auch auf ihren Produktions-Servern und allen Personal-Computern. Unsere Lösung blockiert auf Wunsch Änderungen oder die Ausführung und alarmiert diesbezügliche Unregelmässigkeiten mit detaillierten Angaben aufgrund von vorher definierten Whitelists.
System-Änderungen registrieren	Unsere Lösungen überwachen alle Systemkonfigurationen (aktive Netzwerkkomponenten sowie Server, Clients, Steuerungen usw.) und stellen sicher, dass diese Ihren Richtlinien entsprechen.
Melden und Alarmieren	Unsere Lösungen melden alle Unregelmässigkeiten mit Hilfe eines zentralen Portals, bei dem alle Meldungen zusammenlaufen. Selbstverständlich können alle bestehenden Systeme wie Ticket-System, Change-Management, Alarmierungs-Systeme usw. mit einbezogen werden.

Unsere Partnerschaften

HIRSCHMANN
A BELDEN BRAND

secXTREME
Information Security

TOFINO SECURITY
A BELDEN BRAND

FORTINET

tripwire
CONFIDENCE: SECURED